REMARKS

I. ISSUES NOT RELATING TO PRIOR ART

A. CLAIMS 21-23—CLAIM OBJECTIONS

The Office action objected to claims 21-23 and stated the following reason: "as being in improper form because a multiple dependent claim 21-23. See MPEP 608.01(n)." The reason stated is not grammatically complete and applicants cannot determine the objection or how to correct the claims.

MPEP 608.01(n) contains the form language used in the Office action and includes the text **[2]** in the position of "claim 21-23" in the statement of the Office action. The MPEP states that bracket 2 shall be replaced with either "--should refer to other claims in the alternative only--, and/or, --cannot depend from any other multiple dependent claim--." However, neither option is applicable to claims 21-23. First, claims 21-23 are not actually multiple dependent claims. Each of claims 21-23 refers back to only **one claim** (18, 19, and 20, respectively) and then further limits that referenced claim by referring to additional steps or functions that happen to be recited in other claims. Thus, claims 21-23 are ordinary dependent claims.

Even if claims 21-23 are construed as multiple dependent, they refer to other claims in the alternative only and do not depend from any other multiple dependent claims. Therefore, claims 21-23 are stated in proper multiple dependent form. Reconsideration is respectfully requested.

B. CLAIM 19—ENABLEMENT ISSUE

Claim 19 stands rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the enablement requirement. The Office action states, "Please see In re Hyatt ... which discusses the error regarding single means plus function claims." However, claim 19 recites means for determining a user identifier associated with a network device that has caused a security event in a network; means for causing the network device to receive a network address that is selected from a subset of addresses within a specified pool associated with suspected malicious network users; and means for configuring one or more security restrictions with respect to the selected network address. Claim 19 recites three "means," and is not a single means claim. Clarification and reconsideration are respectfully requested.

C. CLAIMS 19, 22, 25—STATUTORY SUBJECT MATTER

Claims 19, 22, and 25 stand rejected under 35 U.S.C. § 101 as allegedly directed to non-statutory subject matter. The Office action contends that claims 19, 22, and 25 "lack the necessary physical articles or objects to constitute a machine or a manufacture ... they are clearly not a series of steps or acts to be a process nor are they a ... composition of matter ...at best, functional descriptive material *per se*."

This is incorrect. Each of claims 19, 22, and 25 recites an apparatus. An apparatus is a machine, and a machine is statutory subject matter. Each of claims 19, 22, and 25 recites "means" for performing specified functions. The disclosure encompasses physical means for performing the disclosed functions. For example, paragraphs 55 to 64 of the specification describe using computer memory loaded with instructions, computer-readable data storage media such as volatile memory or non-volatile memory encoded or loaded with instructions, hard-wired circuitry (paragraph 57), or a combination of hard-wired circuitry and encoded instructions. The physical means also may include server computers and client computers (paragraph 62-63). Thus, the disclosure is not limited to functional descriptive material (such as computer instructions printed on a page) *per se*.

Because the disclosure describes structural means for performing the specified functions, each of claims 19, 22, and 25 recites statutory subject matter. Reconsideration is respectfully requested.

II. ISSUES RELATING TO PRIOR ART

A. CLAIMS 1, 2, 9-14, 17-26—FREUND

Claims 1, 2, 9-14, and 17-26 stand rejected under 35 U.S.C. § 102(e) as allegedly anticipated by Freund U.S. Pat. No. 5,987,611. The rejections are respectfully traversed.

A rejection under §102 is traversed if the claims recite one or more features, elements, steps or limitations that are not found in the cited reference. Stated another way, the cited reference must teach or disclose each and every feature of the claims, arranged as in the claims. *See Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983). The claims of the present application contain features not found in the reference, and therefore the rejection is overcome.

Claim 1 recites "determining a **user identifier** associated with a network device that has caused a security event in a network." The Office action contends that Freund 12:54-65 shows the quoted feature. This is incorrect. The Office action notes that "an access management application or firewall or filter tracks data packet flow by the source/destination address," but the claim recites determining a **user identifier**, not a source/destination address. A user identifier (e.g., johndoe) is quite different from a source/destination address (e.g., 255.12.24.2). A conventional firewall or filter cannot determine a user identifier associated with a network device that has caused a security event. At most, a firewall or filter can identify a network address (IP address) that is attempting to send traffic on a particular port. Freund has no description of determining a user identifier of someone who caused a security event in a network using Freund's access management application, firewall or filter.

Claim 1 recites "**causing the network device to acquire a new network address** that is selected from a subset of addresses within a specified pool associated with suspected malicious network users." Support is found at least in paragraphs 37-45 of applicants' specification (and original claim 15, so no new search is required). The Office action contends that the quoted feature is found in Freund 12:66-67 and 13:1-22 and states that the "access management application or firewall or packet filter will have a data base or table that is predefined with what particular malicious addresses to look for with particular network users." The Office action appears to overlook or ignore the claimed feature of **causing the network device to receive (acquire) an (new) address**, and the claim has been clarified solely for that reason. Claim 1 causes the network device associated with a security event to acquire a new network address when the security event has been identified. The access management application or firewall or packet filter of Freund provides no way to **assign a new address, or cause a network device to**

receive or acquire a new address, when a security event is identified. At most, Freund can implement rules that block traffic at a firewall or filter, but the address of the firewall or filter—and the client computer that is the source of the problem—remains unchanged. Applicants have an approach that is entirely new with respect to Freund in which devices are essentially quarantined by forcing acquisition of an address within a specified pool that is only for suspected malicious users or devices. Applicants' approach is not within the scope of any reasonable reading of Freund, which only describes conventional firewall or filter rules.

For all these reasons, Freund does not anticipate claim 1. Each of the other independent claims (14, 18, 19, 20, 24, 25, and 26) recites the features that are quoted and discussed above. Therefore, Freund does not anticipate claims 14, 18, 19, 20, 24, 25, or 26 for the same reasons given above for claim 1. Applicants respectfully submit that claims 1, 14, 18, 19, 20, 24, 25, and 26 are allowable over the art of record and are in condition for allowance.

Each of claims 2, 9-13, 17, 21, and 22 depends directly or indirectly from claim 1, 14, 18, 19, or 20 and thus includes each and every feature of the base independent claim. Therefore, each of claims 2, 9-13, 17, 21, and 22 is allowable for the reasons given above with respect to claims 14, 18, 19, and 20.

In addition, each of claims 2, 9-13, 17, 21, and 22 recites independent subject matter that Freund does not anticipate. For example, claim 9 recites that configuring security restrictions comprises "modifying an internet protocol (IP) access control list (ACL) associated with a port that is coupled to the network device to permit entry of IP traffic from only the selected network address." The Office action (at pp. 5-6) appears to regard the claimed feature as ordinary ACL permit/deny address management. However, close reading of the complete claimed combination reveals a completely counter-intuitive approach. As claimed, traffic from a device associated with a security event is **permitted**, not denied. Conventional firewalls and filters would **block** traffic from a malicious device. In the claim, the traffic can be **permitted** because the **selected network address** (from the specified pool for malicious users only) is used, and the system "knows" that this address is subject to the security restrictions recited in the last clause of claim

1. Freund has no suggestion to **permit** entry of traffic from a device that has caused a security event. Therefore, claim 9 is allowable. Reconsideration is respectfully requested.

Claim 10 is similar to claim 9 but recites modifying a MAC ACL rather than an IP ACL. Claim 10 is allowable for the same reasons set forth above for claim 9.

Claim 17 is similar to claim 9 and claim 10, and recites modifying both an IP ACL and a MAC ACL. Claim 17 is allowable for the same reasons set forth above for claim 9.

B. CLAIMS 3-8, 15, 16—FREUND IN VIEW OF HANSON

Claims 3-8, 15, and 16 stand rejected under 35 U.S.C. 103(a) as allegedly unpatentable over Freund in view of Hanson U.S. Patent Publication 2002/0098840. The rejections are respectfully traversed.

Each of claims 3-8, 15, and 16 depends directly on indirectly on one of claim 1 and 14 and thus includes each and every feature of the base independent claim. Therefore, each of claims 3-8, 15, and 16 is allowable for the reasons given above with respect to claims 3-8, 15, and 16.

The claims are also allowable over a combination of Freund and Hanson because Hanson does not disclose the subject matter that is actually recited in the claims, and the Office action does not apply any prior art whatsoever to the complete subject matter that is actually recited in the claims.

For example, claim 3 recites in part, "causing the network device to acquire the new network address comprises resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP." At page 18, the Office action admits that "Freund does not appear to explicitly disclose" the quoted feature. The Office action then states that "Hanson discloses network device obtains a network address by DHCP," citing paragraph 304. However, merely obtaining a network address by DHCP is not what is actually claimed. The claim recites **causing the network device to acquire the new network address comprises resetting a port that is coupled to the network device to prompt a user to command the network device to request a new network address**. The Office action asserts **no evidence** to show that this feature is found in Hanson or any other art. It is not in paragraph 304, which describes DHCP generally and without any application to network security or use to control devices that have caused security events. Therefore, the Office action fails to state a *prima facie* case of unpatentability of claim 3, and the rejection should be withdrawn.

For claims 4 to 8, the Office action identifies no part of Hanson or any other reference that shows the complete subject matter that is claimed. For example, claim 4 recites that "causing the network device to acquire the new network address comprises issuing a DHCP FORCE_RENEW message to the network device"; claim 5 recites that "causing the network device to acquire the new network address comprises prompting the network device to request a new network address using DHCP"; claim 6 recites that "causing the network device to acquire the new network address comprises waiting for expiration of a lease for a current network address of the network device"; claim 7 recites that "causing the network device to acquire the new network address comprises the step of providing the network device with an IP address that is selected from a plurality of IP addresses within a special IP subnet"; and claim 8 recites the subject matter of claim 7 and also "publishing information describing characteristics of the special IP subnet to network service providers." The Office action makes **no attempt** to identify any of these specific claim features in Hanson or any other reference. None of the features is in paragraph 304 of Hanson. Therefore, the Office action fails to state a *prima facie* case of unpatentability of claim 3, and the rejection should be withdrawn.

Further, notwithstanding the fact that neither Freund nor Hanson discloses the above-quoted features of claims 3-8, 15, and 16, nothing in Freund or Hanson teaches or suggests combining their respective teachings. The access management application or firewall or packet filter of Freund provides no way to **assign a new address, or cause a network device to receive or acquire a new address**, when a security event is identified. At most, Freund can implement rules that block traffic at a firewall or filter, but the address of the firewall or filter—and the client computer that is the source of the problem—remains unchanged. Thus, any combination of Hanson with Freund would only provide for **initially** assigning addresses to network devices using conventional DHCP, but not using address re-assignment, port resetting, forced renewal of leases, or any other use of DHCP to isolate or quarantine a network device in response to identifying a security event. Any such combination would not provide the complete combination that is claimed.

The Court of Appeals for the Federal Circuit observed in *In re Dembiczak*, 50 USPQ.2d 1617 (Fed. Cir. 1999), (citing *Gore v. Garlock*, 220 USPQ 303, 313 (Fed. Cir. 1983)), "it is very easy to fall victim to the insidious effect of the hindsight syndrome where that which only the inventor taught is used against its teacher." *Id.* The Federal Circuit stated in *Dembiczak* "that the best defense against subtle but powerful attraction of a hindsight-based obviousness analysis is rigorous application of the requirement for a showing of the teaching or suggestion to combine prior art references." *Id.* Thus, the Federal Circuit explains that a proper obviousness analysis requires "***particular factual findings*** regarding the locus of the suggestion, teaching, or motivation to combine prior art references." *Id.* (emphasis added).

In particular, the Federal Circuit states: "We have noted that evidence of a suggestion, teaching, or motivation to combine may flow from the prior art references themselves, the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved…although 'the suggestion more often comes from the teachings of the pertinent references'…The range of sources available, however, does ***not diminish the requirement for actual evidence***. That is, the ***showing must be clear and particular***…Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" *Id.* (emphasis added; internal citations omitted).

Neither Freund nor Hanson show any suggestion, teaching, or motivation to combine their teachings. The rationale provided at page 19 of the Office action, second paragraph—that it would have been obvious "to allow the network device to obtain a new network address from a pool of addresses that is associated with malicious users, and allow network security to analyze it separately from the rest of the network traffic," does not come from Freund or Hanson but must be based on hindsight with the benefit of applicants' disclosure. The second rationale proposed in the Office action is not actually supported in Hanson paragraph 0457, which describes completely different issues.

For all these reasons, claims 3-8, 15, and 16 are allowable over Freund in view of Hanson. Reconsideration is respectfully requested.

C. NEW CLAIMS 27-31

Five new claims 27-31 correspond to selected ones of dependent claims 2-14 but are expressed in apparatus format dependent upon claim 20 or claim 26. The new claims are allowable for the same reasons given above for the corresponding method claims. Extra claim fees are submitted concurrently herewith. Favorable consideration is respectfully requested.

III. CONCLUSIONS

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

/ChristopherJPalermo#42056
Christopher J. Palermo
Reg. No. 42056

Date: August 21, 2007

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076